The opinion in support of the decision being entered today was not written for publication in a law journal and is not binding precedent of the Board.

Paper No. 24

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SATOSHI HOSHINO

Appeal No. 2002-0108
Application No. 09/200,981

HEARD: MARCH 18, 2003

Before KRASS, FLEMING and BARRY, Administrative Patent Judges.

KRASS, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the final rejection of claims 1-8.

The invention is directed to a system for authenticating personal identification in order to allow a user to obtain access to a client terminal. The client terminal is connected to a

server via a network, with the server including a database that stores personal information regarding a user ID number and a user fingerprint. When a user desires to gain access to the client terminal, the user inserts an IC card including relevant ID information into an IC card reader at the client terminal and also places his/her finger on a fingerprint sensor at the client terminal.

An authenticator at the client terminal compares information corresponding to the sensed fingerprint to information obtained from the IC card. If a match occurs, an authentication signal is produced. Then, only if there is a match, the client terminal provides the sensed fingerprint information, the IC card information and the authentication signal, to the server.

Once the server receives this information from the client terminal, it is compared with stored personal information from the database. If there is a match, then the server authorizes use of the client terminal by the user.

By sending information to the server *only* when there is a match at the client terminal, a reduction in load carried by the server and the network is alleged to occur.

Representative independent claim 1 is reproduced as follows:

1. A system for authenticating personal identification, comprising:

a server including a computer whose users are limited, said server having a database storing information related to ID numbers assigned to said users and information related to fingerprints of said users;

an IC card storing personal information including information related to an ID number of the card owner and information related to a fingerprint of the card owner;

a client terminal in communication with said server, said client terminal including a card reader for reading the stored personal information on said IC card, and a fingerprint sensor for sensing a fingerprint of the client terminal user;

said client terminal comprising:

an authenticator that compares the sensed fingerprint information of the client terminal user with the stored fingerprint information of the card owner and produces an authentication signal if the sensed fingerprint information matches the stored fingerprint information; and

a transmitter that transmits personal information including the sensed fingerprint information and the authentication signal to said server only if the authentication signal is produced by the authenticator; and

said server comprising:

an authorizer that compares the transmitted personal information of the card owner with the stored personal information on the database and produces an authorization signal if the transmitted personal information matches the stored information on the database, thereby to give the client terminal user an access to said computer of said server,

wherein said server does not receive any information from the client terminal if the authenticator determines that the sensed fingerprint information of the client terminal user does not match with the stored fingerprint information of the card owner.

The examiner relies on the following references:

Fujieda et al. [Fujieda]	5,446,290	Aug. 29, 1995
Lane	5,623,552	Apr. 22, 1997
Maes et al. [Maes]	6,016,476	Jan. 18, 2000
		(filed Jan. 16, 1998)

Claims 1-8 stand rejected under 35 U.S.C. § 103. As evidence of obviousness, the examiner offers Lane and Maes with regard to claims 1-3 and 5-8, adding Fujieda with regard to claim 4.

Reference is made to the briefs and answer for the respective positions of appellant and the examiner.

OPINION

We REVERSE.

Each of independent claims 1 and 5 requires an authentication at *both* the client terminal *and* at the server. Thus, an authenticator at the client terminal first compares sensed fingerprint information with stored fingerprint information on an IC card. If there is a match, and only if there is a match, the client terminal produces an authentication signal and that authentication signal is transmitted to the server, along with the sensed fingerprint information and other personal information. There is then *another* authentication process at the server, whereby the server compare the transmitted personal information of the card owner with personal information stored in the server database. The server then produces its own authentication signal if the transmitted personal information matches the stored information in the database. The server authentication signal permits the client terminal user access to the server computer. Thus, access is denied if the server determines that the sensed fingerprint information of the client

terminal user does not match the stored fingerprint information of the card owner.

Lane teaches a self-authenticating card which includes a fingerprint sensor for authenticating the identity of a user, by comparing information related to a sensed fingerprint with the stored fingerprint information. An authentication signal is produced if there is a match. Lane's authentication system takes place at a client terminal but there is no second authentication at a server.

Maes performs an authentication at a server (e.g., box 108 in the flowchart of Figure 4) but there is no authentication at a client terminal since all verification is performed at the server.

The examiner attempts to combine these teachings in order to arrive at the claimed subject matter "in order to increase the level of security for user verification whereby the user is verified at both the terminal, the financial institution server and is granted authorization for executing the transactions when

successfully being verified by both the terminal and the server (col. 13, lines 20-29)" [answer-page 7].

While providing an additional level of security may be a valid goal of an artisan, the examiner's rationale, in our view, is unconvincing as to what would have led the artisan to take an authentication at the client terminal (Lane) and an authentication at a server (Maes) and combine them in order to first authenticate at the client terminal, by comparing a sensed fingerprint with fingerprint information contained on an IC card, and send information, including an authentication signal, to a server only upon a match of fingerprint information whereby, upon receipt of such information, the server then compares the fingerprint information sensed at the client terminal with fingerprint information stored in a database at the server so as to determine if the fingerprint sensed at the client terminal belongs to the owner of the IC card. The desire, per se, to provide an additional level of security would not have led to the specific combination of elements and interrelationships set forth by the subject matter of independent claims 1 and 5.

Accordingly, since the examiner has not convinced us of an adequate motivation to combine the teachings of Lane and Maes, we will not sustain the rejection of claims 1-3 and 5-8 under 35 U.S.C. § 103. Since Fujieda does not provide for the deficiencies of the primary references, we also will not sustain the rejection of claim 4 under 35 U.S.C. § 103.

The examiner's decision is reversed.

REVERSED

ERROL A. KRASS Administrative Patent Judge	)
MICHAEL R. FLEMING Administrative Patent Judge	) BOARD OF PATENT) APPEALS AND) INTERFERENCES
LANCE LEONARD BARRY Administrative Patent Judge	)

EAK/dal

FOLEY & LARDNER
3000 K STREET NW
SUITE 500
WASHINGTON, DC 20007-8696